

Quassel IRC - Bug #686

fails do connect to OFTC with SSL

05/03/2009 01:55 PM - DeepDiver

Status:	Rejected	Start date:	05/03/2009
Priority:	Normal	Due date:	
Assignee:	EgS	% Done:	0%
Category:	Quassel Core	Estimated time:	0.00 hour
Target version:		OS:	Linux
Version:	0.4.0		

Description

this is reported by a debian user: <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526590>

Quassel is not able to connect to OFTC when the SSL option in the irc.oftc.net server configuration is enabled. Changing it from the default of SSL3 to TLSv1 doesn't make a difference, either. The error message which appears in the network window is:

```
[21:31:17] * Connecting to irc.oftc.net:6667...
[21:31:17] * Connection failure: Error during SSL
handshake:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version
number
[21:31:17] * Connection failed. Cycling to next Server
```

OTOH, when using openssl's s_client works:

```
$ openssl s_client -connect irc.oftc.net:6697
[...]
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
[...]
```

or even asking for SSL3:

```
$ openssl s_client -connect irc.oftc.net:6697 -ssl3
[...]
SSL-Session:
Protocol : SSLv3
Cipher : AES256-SHA
[...]
```

but, when trying to use SSL2:

```
$ openssl s_client -connect irc.oftc.net:6697 -ssl2
CONNECTED
write:errno=104
```

I was able to reproduce this with the monolithic client as well

THX Tom

History

#1 - 05/15/2009 01:06 PM - DeepDiver

Ping! ;-))

#2 - 05/22/2009 01:37 AM - EgS

- Status changed from New to Rejected

- Assignee set to EgS

PONG! ;)

And sorry for the late reply.

OFTC offers regular IRC connections on port 6667 and for SSL enabled clients on port 6697 (see: <http://www.oftc.net/oftc/>).

So if you want to connect via SSL to OFTC you have to change the port number from 6667 to 6697. As each IRC network has different SSL ports we cannot change the port automatically when switching to SSL.

#3 - 05/23/2009 01:38 PM - DeepDiver

Oh - I'm sorry.

I didn't check the port number.

THX Tom